ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

Кафедра

«Криптология и кибербезопасность»

Контрольная работа №1

«Поиск уязвимостей по открытым источникам»

Исполнитель:

студент гр. Б19-515 Щербакова А. Е.

подпись,

дата

Преподаватель: Анисимов Д.В.

подпись,

дата

Москва — 2023

1 Введение

Для анализа уязвимостей выбраны следующие пакеты: sudo 1.8.20 и Perl 5.26.3. Для поиска уязвимостей использовался сайт https://nvd.nist.gov/products/cpe/search

2 Пакет sudo 1.8.20

Найдено 10 уязвимостей: CVE-2023-22809, CVE-2022-43995, CVE-2021-3156, CVE-2021-23240, CVE-2021-23239, CVE-2019-18634, CVE-2019-18684, CVE-2019-14287, CVE-2017-1000368, CVE-2017-1000367.

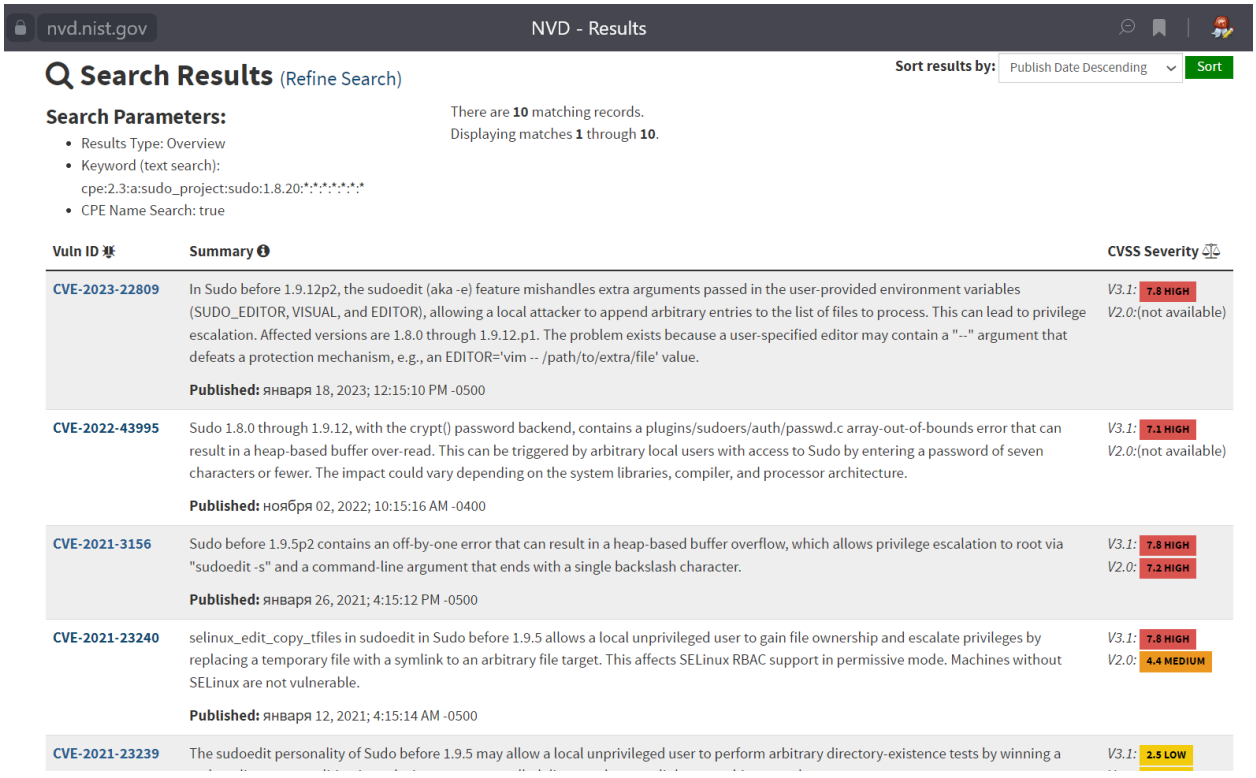

Рисунок 1 – Уязвимости пакета sudo 1.8.20 (часть 1)

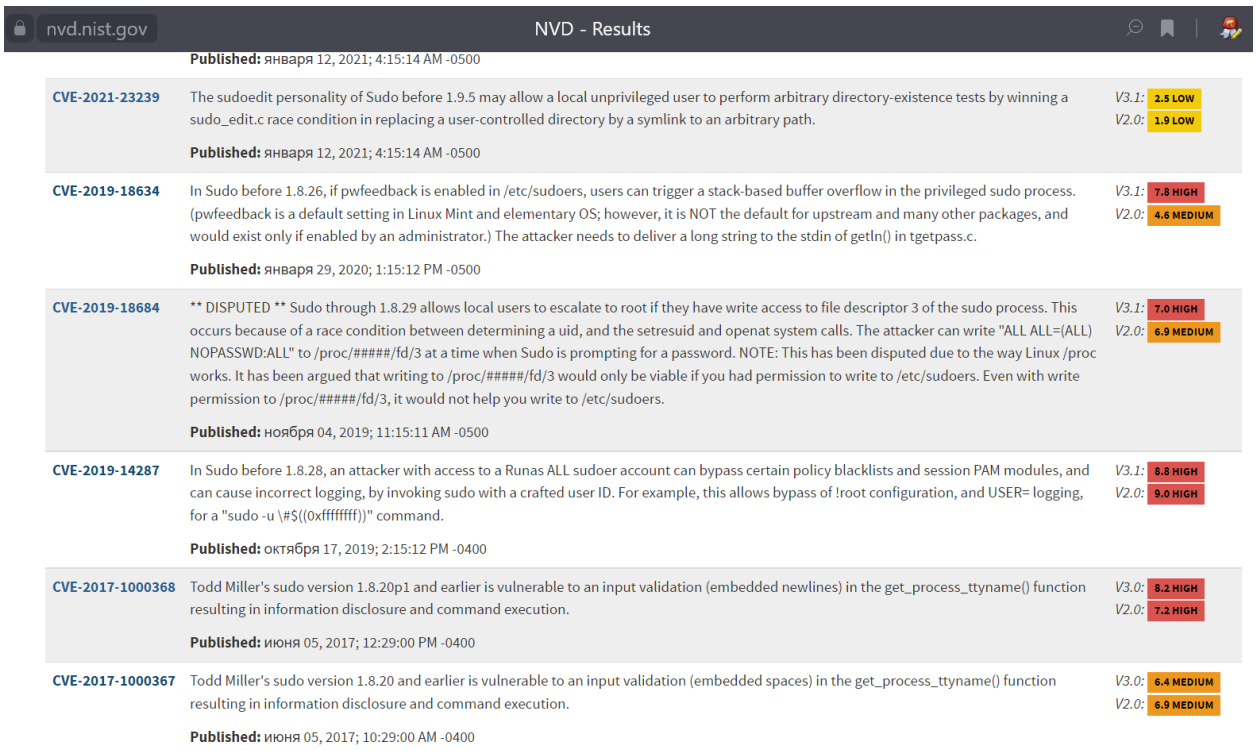

Рисунок 2 – Уязвимости пакета sudo 1.8.20 (часть 2)

Далее скриншотов по каждой уязвимости не приложено, так как их слишком много, а их содержание как раз и представлено в таблице.

Способ устранения для всех уязвимостей – обновиться до исправленной версии пакета.

Таблица 1 – Описание уязвимостей пакета sudo 1.8.20.

Название уязвимости	Описание и вектор атаки	Критичность	Устранение
CVE-2022-43995	Sudo с 1.8.0 по 1.9.12 с серверной частью пароля crypt() содержит ошибку plugins/sudoers/auth/passwd.c, выходящую за пределы массива, которая может привести к переполнению буфера на основе кучи. Это может быть вызвано произвольными локальными пользователями, имеющими доступ к Sudo, путем ввода пароля из семи символов или	CVSS 3.x – High (7.1) CVSS 2.0 – not available	Исправлена в версии sudo 1.8.29-4 и 1.9.13

	менее. Влияние может варьироваться в зависимости от системных библиотек, компилятора и архитектуры процессора.		
CVE-2021-3156	Sudo до 1.9.5p2 содержит случайную ошибку, которая может привести к переполнению буфера на основе кучи, что позволяет повысить привилегии root с помощью "sudoedit -s" и аргумента командной строки, который заканчивается одним символом обратной косой черты. Эксплойт: https://github.com/worawit/CVE-2021-3156	CVSS 3.x – High (7.8) CVSS 2.0 – not available	Ошибка исправлена в sudo 1.8.32 и 1.9.5p2.
CVE-2023-22809	В Sudo до 1.9.12p2 функция sudoedit (она же -e) неправильно обрабатывает дополнительные аргументы, передаваемые в пользовательских переменных среды (SUDO_EDITOR, VISUAL и EDITOR), позволяя локальному злоумышленнику добавлять произвольные записи в список файлов для обработки. Это может привести к повышению привилегий. Затронутые версии - с 1.8.0 по 1.9.12.p1. Проблема существует из-за того, что указанный пользователем редактор может содержать аргумент "--", который отключает механизм защиты, например, значение EDITOR='vim -- /path/to/extra/file'. Эксплойт: https://github.com/M4fiaB0y/CVE-2023-22809	CVSS 3.x – High (7.8) CVSS 2.0 – High (7.2)	Исправлена в версии sudo 1.9.12p2

CVE-2021-23240	selinux_edit_copy_tfiles в sudoedit в Sudo до версии 1.9.5 позволяет локальному непривилегированному пользователю получить право собственности на файл и повысить привилегии, заменив временный файл символической ссылкой на произвольный целевой файл. Это влияет на поддержку SELinux RBAC в разрешающем режиме. Машины без SELinux не уязвимы.	CVSS 3.x – High (7.8) CVSS 2.0 – Medium (4.4)	Исправлена в версии sudo 1.9.5
CVE-2021-23239	Идентификатор sudoedit в Sudo до версии 1.9.5 может позволить локальному непривилегированному пользователю выполнять тесты на существование произвольного каталога, выиграв условие гонки sudo_edit.c при замене каталога, контролируемого пользователем, символической ссылкой на произвольный путь.	CVSS 3.x – Low (2.5) CVSS 2.0 – Low (1.9)	Исправлена в версии sudo 1.9.5
CVE-2019-18634	В Sudo до версии 1.8.26, если pwfeedback включен в /etc/sudoers, пользователи могут вызвать переполнение буфера на основе стека в привилегированном процессе sudo. (pwfeedback - это настройка по умолчанию в Linux Mint и elementary OS; однако она не используется по умолчанию для upstream и многих других пакетов и будет существовать только в том случае, если включена администратором.) Злоумышленнику необходимо передать длинную строку в	CVSS 3.x – High (7.8) CVSS 2.0 – Medium (4.6)	Исправлена в версии sudo 1.8.26

	stdin функции getting() в tgetpass.c. Эксплойт: https://github.com/Plazmaz/CVE-2019-18634		
CVE-2019-18684	Sudo до 1.8.29 позволяет локальным пользователям перейти на root, если у них есть доступ на запись к файловому дескриптору 3 процесса sudo. Это происходит из-за состояния гонки между определением uid и setresuid и open при системных вызовах. Злоумышленник может записать "ALL ALL=(ALL) NOPASSWD:ALL" в /proc/#####/fd/3 в то время, когда Sudo запрашивает пароль. ПРИМЕЧАНИЕ: Это было оспорено из-за того, как работает Linux / proc. Утверждалось, что запись в /proc /#####/fd/3 была бы жизнеспособной только в том случае, если бы у вас было разрешение на запись в /etc /sudoers. Даже с разрешением на запись в /proc /#####/fd /3 это не помогло бы вам записывать в /etc/sudoers.	CVSS 3.x – High (7.0) CVSS 2.0 – Medium (6.9)	Исправлена в версии sudo 1.8.29
CVE-2019-14287	В Sudo до версии 1.8.28 злоумышленник, имеющий доступ к учетной записи Runas ALL sudoer, может обойти определенные черные списки политик и модули PAM сеанса и вызвать неправильное ведение журнала, вызвав sudo с созданным идентификатором пользователя. Например, это позволяет обходить !root configuration и USER= logging для команды "sudo -u \#$((0xffffffff))".	CVSS 3.x – High (8.8) CVSS 2.0 – High (9.0)	Исправлена в версии sudo 1.8.28

	Эксплойт: https://www.sudo.ws/security/advisories/minus_1_uid/		
CVE-2017-1000368	Sudo Тодда Миллера версии 1.8.20p1 и более ранних уязвим для проверки ввода (встроенные новые строки) в функции get_process_ttyname(), что приводит к раскрытию информации и выполнению команды.	CVSS 3.x – High (8.2) CVSS 2.0 – High (7.2)	Исправлена в версии sudo 1.8.20p2
CVE-2017-1000367	Sudo от Тодда Миллера версии 1.8.20 и более ранних версий уязвим для проверки входных данных (встроенные пробелы) в функции get_process_ttyname(), что приводит к раскрытию информации и выполнению команды.	CVSS 3.x – Medium (6.4) CVSS 2.0 – Medium (6.9)	Исправлена в версии sudo 1.8.20p2

2 Пакет Perl 5.26.3

Найдено 9 уязвимостей: CVE-2021-36770, CVE-2020-12723, CVE-2020-10878, CVE-2016-1246, CVE-2011-3599, CVE-2011-2201, CVE-2010-1168, CVE-2009-1884, CVE-2009-0663.

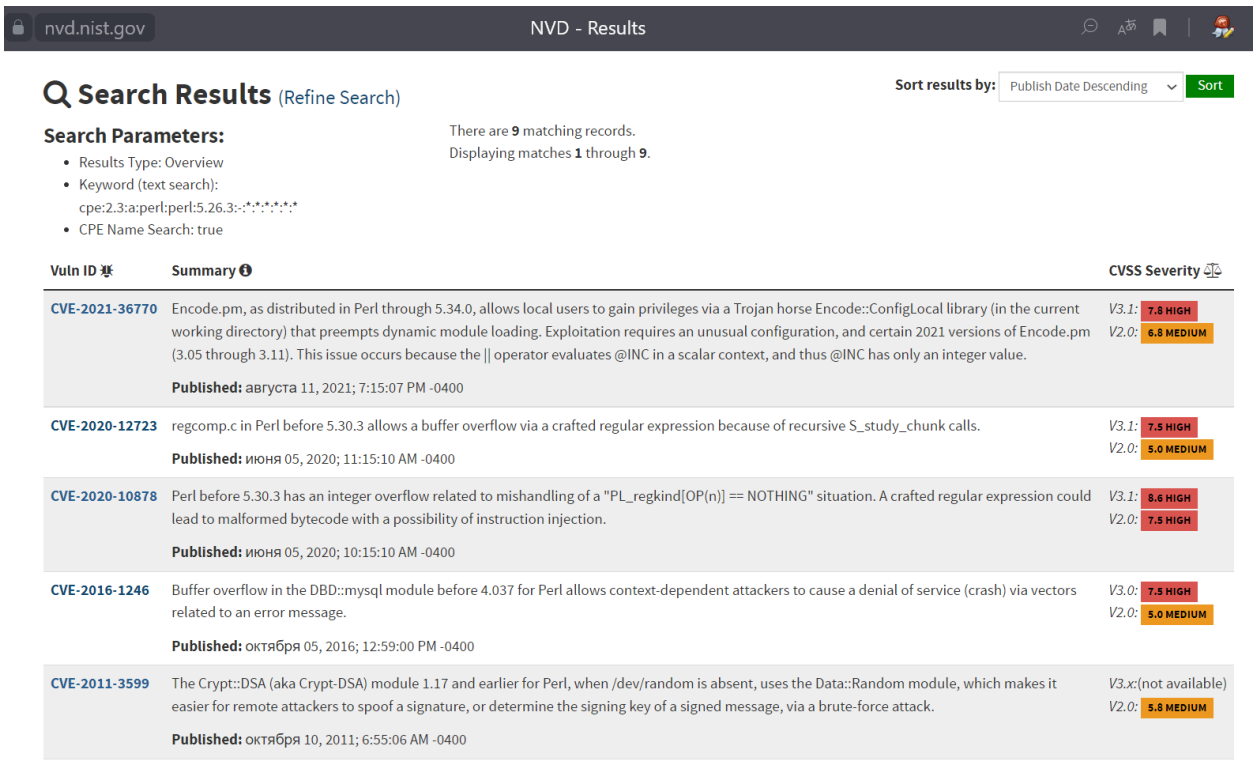

Рисунок 3 – Уязвимости пакета Perl 5.26.3 (часть 1)

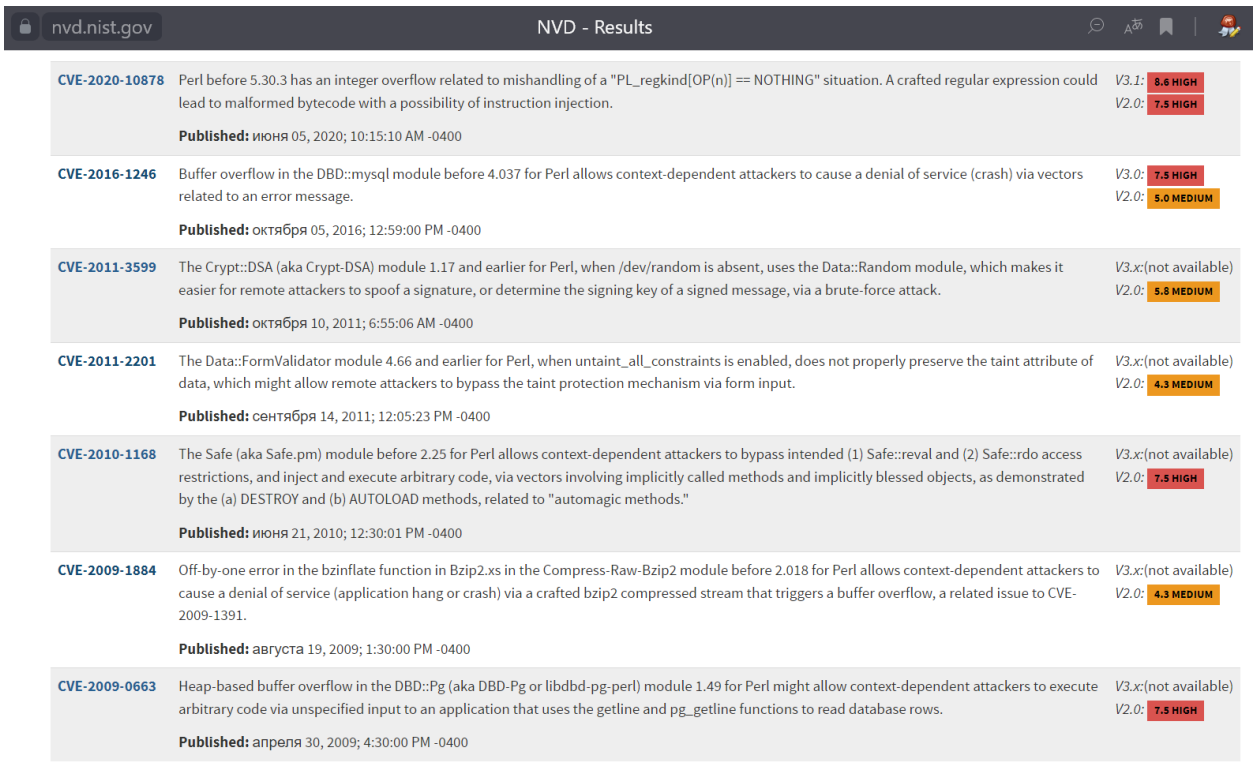

Рисунок 4 – Уязвимости пакета sudo 5.26.3 (часть 1)

Таблица 2 – Описание уязвимостей пакета Perl 5.26.3.

Название уязвимости	Описание и вектор атаки	Критичность	Устранение
CVE-2021-36770	Encode.pm , распространяемый на Perl до версии 5.34.0, позволяет локальным пользователям получать привилегии с помощью троянского коня Encode::ConfigLocal library (в текущем рабочем каталоге), который предотвращает загрузку динамического модуля. Эксплуатация требует необычной конфигурации, и некоторые версии 2021 года Encode.pm (с 3.05 по 3.11). Эта проблема возникает из-за того, что оператор || вычисляет @INC в скалярном контексте, и, таким образом, @INC имеет только целочисленное значение.	CVSS 3.x – High (7.8) CVSS 2.0 – Medium (6.8)	Исправлена в версии 5.34.0
CVE-2020-12723	regcomp.c в Perl до версии 5.30.3 допускает переполнение буфера с помощью созданного регулярного выражения из-за рекурсивных вызовов S_study_chunk.	CVSS 3.x – High (7.5) CVSS 2.0 – Medium (5.0)	Исправлена в версии 5.30.3
CVE-2020-10878	Perl до версии 5.30.3 имеет переполнение целых чисел, связанное с неправильным обращением с ситуацией "PL_regkind[OP(n)] == NOTHING". Созданное регулярное выражение может привести к искаженному байт-коду с возможностью внедрения команд.	CVSS 3.x – High (7.5) CVSS 2.0 – High (8.6)	Исправлена в версии 5.30.3
CVE-2016-1246	Переполнение буфера в модуле DBD::mysql до версии 4.037 для Perl позволяет контекстно-зависимым злоумышленникам вызывать	CVSS 3.x – High (7.5) CVSS 2.0 – Medium (5.0)	Обновление версии mysql до 4.41.0

	отказ в обслуживании (сбой) с помощью векторов, связанных с сообщением об ошибке.		
CVE-2011-3599	Модуль Crypt::DSA (он же Crypt-DSA) 1.17 и более ранних версий для Perl, когда /dev/random отсутствует, использует модуль Data::Random, который облегчает удаленным злоумышленникам подделку подписи или определение ключа подписи подписанного сообщения с помощью брутфорса.	CVSS 3.x – not available CVSS 2.0 – Medium (5.8)	Исправлено в версии: perl-Crypt-DSA-1.17-10.*, perl-Crypt-DSA-0.14-8.el5
CVE-2011-2201	Модуль Data::FormValidator 4.66 и более ранних версий для Perl, когда включен параметр untaint_all_constraints, неправильно сохраняет атрибут заражения данных, что может позволить удаленным злоумышленникам обойти механизм защиты от заражения через ввод формы.	CVSS 3.x – not available CVSS 2.0 – Medium (4.3)	Исправлено в версиях libdata-formvalidator-perl/4.66-3, libdata-formvalidator-perl/4.66-1+squeeze1
CVE-2010-1168	Safe (он же Safe.pm) модуль до 2.25 для Perl позволяет контекстно-зависимым злоумышленникам обходить предполагаемые (1) ограничения доступа Safe::reval и (2) Safe::rdo, а также вводить и выполнять произвольный код с помощью векторов, включающих неявно вызываемые методы и неявно благословленные объекты, как продемонстрировано методы (a) DESTROY и (b) AUTOLOAD, относящиеся к "автоматическим методам".	CVSS 3.x – not available CVSS 2.0 – High (7.5)	Обновитесь до Safe.pm версия v2.25 или выше.
CVE-2009-1884	Случайная ошибка в функции bzinflate в Bzip2.xs в модуле Compress-Raw-Bzip2 до версии 2.018 для Perl позволяет	CVSS 3.x – not available CVSS 2.0 –	Исправлена в версии perl-Compress-

	контекстно-зависимым злоумышленникам вызывать отказ в обслуживании (зависание или сбой приложения) через созданный сжатый поток bzip2, который вызывает переполнение буфера, что является проблемой, связанной с CVE-2009-1391.	Medium (4.3)	Raw-Bzip2 2.0.18
CVE-2009-0663	Переполнение буфера на основе кучи в модуле 1.49 DBD::Pg (он же DBD-Pg или libdbd-pg-perl) для Perl может позволить контекстно-зависимым злоумышленникам выполнять произвольный код через неопределенный ввод в приложение, которое использует функции getline и pg_getline для чтения строк базы данных.	CVSS 3.x – not available CVSS 2.0 – High (7.5)	Исправлена в версии 1.50 DBD::Pg